Cuadro de tratamiento de riesgos Implementado desde el [fecha] hasta el [fecha]

Activos / amenazas / vulnerabilidades						Valores antes del tratamiento		
Cantidad	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo
1	aplicación de software	gerente de TI	errores de aplicación	falta de control de datos de entrada y salida	gerente de TI	2	1	3
2	enlaces de comunicación	gerente de TI	violación de seguridad	Falta o mala implementación de la auditoría interna	gerente de TI	3	1	3
3	application software	gerente de TI	errores de aplicación	conexiones de red pública desprotegidas	gerente de TI	3	1	3
4	oficinas	gerente de instalaciones	interrupción del suministro	ubicación sensible a desastres naturales	gerente de instalaciones	2	1	3
5	enlaces de comunicación	gerente de TI	Fallo en el equipo	ubicación sensible a fugas de agua	gerente de TI	3	1	3

Tratamiento del riesgo		Valores después del tratamiento		
Elección de opciones	Medios de implementación	Consecuencia	Probabilidad	Riesgo
2. Transferencia de riesgos a un t	A.5.20 Abordar la seguridad de la ir	2	0	2
3. Elección de controles	A.5.22 Supervisión, revisión y gestió	0	0	0
3. Transferencia de riesgos a terc	A.5.20 Abordar la seguridad de la i	0	0	0
1. Elección de controles	A.7.5 Protección ante amenazas fís	2	0	2
3. Elección de controles	A.7.8 Ubicación y protección del eq	0	0	0
				0
				0
				0
				0
				0
				0
				0
				0
				0
				0
				0

Opciones para el tratamiento de riesgos

1. Elección de controles
2. Transferencia de riesgos a terceros
3. Evitar el riesgo
4. Aceptación del riesgo

Controles de acuerdo al Anexo A de la norma ISO/IEC 27001

A.5.1 Políticas para seguridad de la información
A.5.2 Roles y responsabilidades sobre seguridad de la información
A.5.3 Segregación de deberes
A.5.4 Responsabilidades de la dirección
A.5.5 Contacto con autoridades
A.5.6 Contacto con grupos de interés especial
A.5.7 Inteligencia sobre amenazas
A.5.8 Seguridad de la información en la gestión de proyectos
A.5.9 Inventario de información y otros activos asociados
A.5.10 Uso aceptable de la información y otros activos asociados
A.5.11 Devolución de activos
A.5.12 Clasificación de la información
A.5.13 Etiquetado de la información
A.5.14 Transferencia de la información
A.5.15 Control de acceso
A.5.16 Gestión de identidad
A.5.17 Información de autenticación
A.5.18 Derechos de acceso
A.5.19 Seguridad de la información en las relaciones con los proveedores
A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores
A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
A.5.22 Supervisión, revisión y gestión de cambios de servicios de proveedores
A.5.23 Seguridad de la información para el uso de servicios en la nube
A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
A.5.25 Evaluación y decisión sobre eventos de seguridad de la información
A.5.26 Respuesta a incidentes de seguridad de la información
A.5.27 Aprendizaje a partir de los incidentes en seguridad de la información
A.5.28 Recolección de evidencia
A.5.29 Seguridad de la información durante la interrupción
A.5.30 Preparación de las TIC para la continuidad del negocio
A.5.31 Requisitos legales, estatutarios, reglamentarios y contractuales
A.5.32 Derechos de propiedad intelectual
A.5.33 Protección de registros
A.5.34 Privacidad y protección de IIP
A.5.35 Revisión independiente de seguridad de la información
A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información
A.5.37 Procedimientos operativos documentados
A.6.1 Selección
A.6.2 Términos y condiciones de empleo
A.6.3 Concientización, educación y formación en seguridad de la información
A.6.4 Proceso disciplinario
A.6.5 Responsabilidades después de la terminación o cambio de empleo
A.6.6 Acuerdos de confidencialidad o no divulgación
A.6.7 Trabajo remoto
A.6.8 Reportando de eventos de seguridad de la información
A.7.1 Perímetros de seguridad física
A.7.2 Entrada física
A.7.3 Asegurar oficinas, salas e instalaciones

A.7.4 Monitoreo de seguridad física
A.7.5 Protección ante amenazas físicas y ambientales
A.7.6 Trabajo en áreas seguras
A.7.7 Escritorio y pantalla limpios
A.7.8 Ubicación y protección del equipo
A.7.9 Seguridad de los activos fuera de las instalaciones
A.7.10 Medios de almacenamiento
A.7.11 Utilidades de apoyo
A.7.12 Seguridad del cableado
A.7.13 Mantenimiento de equipo
A.7.14 Eliminación segura o reutilización de equipos
A.8.1 Dispositivos de punto final de usuario
A.8.2 Derechos de acceso privilegiado
A.8.3 Restricción al acceso a la información
A.8.4 Acceso al código fuente
A.8.5 Autenticación segura
A.8.6 Gestión de capacidad
A.8.7 Protección contra malware
A.8.8 Gestión de vulnerabilidades técnicas
A.8.9 Gestión de configuración
A.8.10 Eliminación de información
A.8.11 Enmascaramiento de datos
A.8.12 Prevención de fuga de datos
A.8.13 Copia de seguridad de la información
A.8.14 Redundancia de las instalaciones de procesamiento de información
A.8.15 Registro
A.8.16 Actividades de monitorización
A.8.17 Sincronización de reloj
A.8.18 Uso de programas de utilidad privilegiados
A.8.19 Instalación de software en sistemas operativos
A.8.20 Seguridad en redes
A.8.21 Seguridad de los servicios de red
A.8.22 Segregación de redes
A.8.23 Filtrado web
A.8.24 Uso de criptografía
A.8.25 Ciclo de vida de desarrollo seguro
A.8.26 Requisitos de seguridad de la aplicación
A.8.27 Principios de arquitectura e ingeniería de sistemas seguros
A.8.28 Codificación segura
A.8.29 Prueba de seguridad en desarrollo y aceptación
A.8.30 Desarrollo subcontratado
A.8.31 Separación de los entornos de desarrollo, prueba y producción
A.8.32 Gestión de cambios
A.8.33 Información de prueba
A.8.34 Protección de los sistemas de información durante las pruebas de auditoría